Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems

Nitin Naik[1] and Paul Jenkins[2]

[1]School of Informatics and Digital Engineering, Aston University, United Kingdom
[2]Cardiff School of Technologies, Cardiff Metropolitan University, United Kingdom
Email: n.naik1@aston.ac.uk and pjenkins2@cardiffmet.ac.uk

***Abstract*—Digital identity is the key element of digital transformation in representing any real-world entity in the digital form. To ensure a successful digital future the requirement for an effective digital identity is paramount, especially as demand increases for digital services. Several Identity Management (IDM) systems are developed to cope with identity effectively, nonetheless, existing IDM systems have some limitations corresponding to identity and its management such as sovereignty, storage and access control, security, privacy and safeguarding, all of which require further improvement. Self-Sovereign Identity (SSI) is an emerging IDM system which incorporates several required features to ensure that identity is sovereign, secure, reliable and generic. It is an evolving IDM system, thus it is essential to analyse its various features to determine its effectiveness in coping with the dynamic requirements of identity and its current challenges. This paper proposes numerous governing principles of SSI to analyse any SSI ecosystem and its effectiveness. Later, based on the proposed governing principles of SSI, it performs a comparative analysis of the two most popular SSI ecosystems uPort and Sovrin to present their effectiveness and limitations.**

***Index Terms*—Self-Sovereign Identity; SSI; Principles of SSI; Identity Management System; IDM; Digital Identity; Distributed Ledger; Blockchain; Federated Identity Management; uPort; Sovrin.**

1. Introduction

Digital identity is a precondition to participate in the digital world because it is essential in representing any real-world entity in digital form. As the number and type of entities are increasing, the demand for a digital identity is of greater importance for a successful digital future. Though, it is a complex and challenging field for security experts as it involves several private and sensitive aspects of human life. Several Identity Management (IDM) systems are developed to provide identity and its associated services. Nonetheless, the existing IDMs are still unable to address several important issues related to identity and its management such as sovereignty, storage and access control, security, privacy and safeguarding [1]. Thus, further improvement is required in this area of IDM to address all these issues effectively. With the introduction of blockchain, a new identity management model called Self-Sovereign Identity (SSI) was introduced which aims to address all the above issues [2]. Additionally, it is a peer-to-peer IDM model and does not involve any third-party between the user and organisation.

SSI is an emerging IDM which incorporates several required features to ensure that identity is sovereign, secure, reliable and generic. As SSI is evolving it requires meticulous analysis to determine its effectiveness as a highly acceptable IDM. In the past, numerous governing principles have been proposed for analysing its predecessor federated IDM model [3], [4]. This paper extends the analysis of the federated IDM model by proposing the enhancement of these governing principles to analyse the effectiveness of this emerging SSI IDM model. Later, based on the proposed governing principles of SSI, it performs a comparative analysis of the two most popular SSI ecosystem uPort [5] and Sovrin [6] to present their effectiveness and limitations. The uPort SSI ecosystem is built on the public permissionless blockchain Ethereum [5], and the Sovrin SSI ecosystem is built on the public permissioned blockchain Hyperledger Indy [6].

The rest of the paper is structured as follows: Section 2 elucidates the development of the three IDM Models: Centralised IDM, Federated IDM and Self-Sovereign IDM. Section 3 proposes the numerous governing principles of SSI. Section 4 performs the comparative analysis of uPort and Sovrin based on the proposed governing principles of SSI. Section 5 presents the summary of the paper and related future work.

2. Development of Identity Management (IDM) Models

This section presents the development of three IDM models: Centralised IDM, Federated IDM and Self-Sovereign IDM as shown in Fig. 1.

2.1. Centralised Identity Management Model (IDM 1.0)

The centralised IDM model is the oldest IDM model, in which an organization issues credentials to their users permitting them to use their services. The trust relationship between organisation and user is based on a shared *secret*, in most cases, this is typically a username and password [7]. The user's identity related personally identifiable information

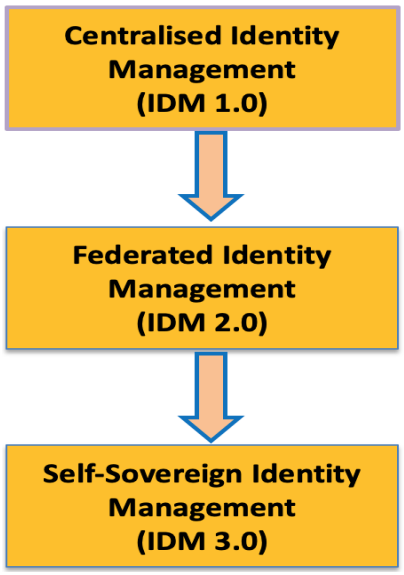

Fig. 1. Development of Identity Management (IDM) Models

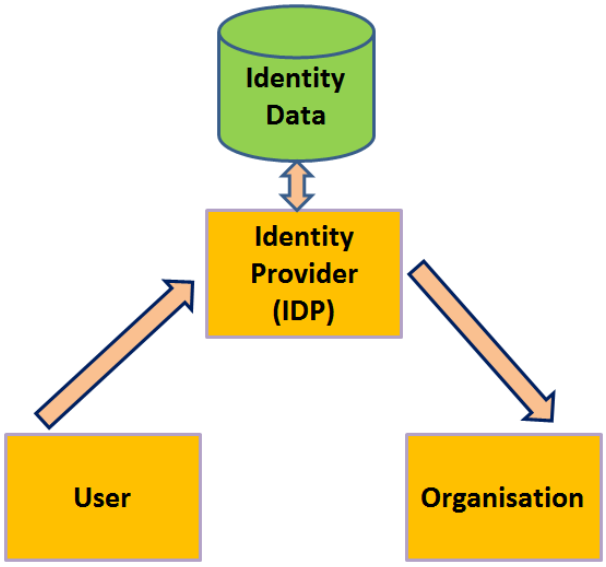

Fig. 3. Federated Identity Management Model (IDM 2.0)

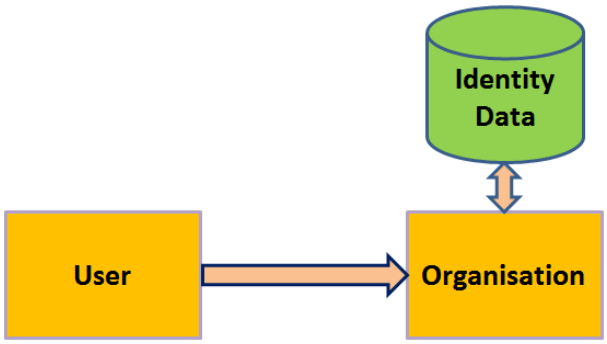

Fig. 2. Centralised Identity Management Model (IDM 1.0)

is always stored and controlled by the organisation (see Fig. 2). Additionally, the user repeats this process and requires separate credentials for each organisation or system, they wish to obtain service from them.

2.2. *Federated Identity Management Model (IDM 2.0)*

This federated IDM model solves two major issues: 1) it removes the organisational burden of managing identity and credentials securely by introducing a third-party IDentity Provider (IDP), which is an additional task alongside the main business operations and 2) it removes the burden from users to manage several identity related credentials for several systems by offering a Single-Sign On (SSO) facility [8], [9]. However, this IDM model has a similar issue in that the abundance of identity related personally identifiable information of a user is held by the IDP (see Fig. 3), and therefore, the user has no control over this information.

2.3. *Self-Sovereign Identity Management Model (IDM 3.0)*

This self-sovereign IDM model is an improvement on the federated IDM model, where it removes the third-party IDP and offers a direct connectivity between a user and organisation. Furthermore, it resolves the main issue of ownership of identity related personally identifiable information of a user by offering its full control through the use of a *Digital Wallet* [10]. The *Digital Wallet* stores all the identity related personally identifiable information which is owned and controlled by a user on the device controlled by the user (see Figs. 4 and 5). SSI assumes three key roles i.e. *Issuer, Holder and Verifier*, in its ecosystem as shown in Fig. 5. An issuer creates and issues credentials to a holder. A holder receives credentials from an issuer, holds it and when required, it shares these credentials with a verifier. A verifier receives and verifies credentials presented by a holder.

This SSI implementation is based on some new standards such as Verifiable Credential (VC) [11] and Decentralized IDentifier (DID) [12] standards which are proposed to create a cryptographically verifiable digital identity that is fully governed by its owner [13], [14]. A VC is used to represent similar information on the Web to that of a physical credential in the real world. The DID is a permanent, universally unique identifier and cannot be taken away from its owner who owns the associated private key, which is completely different from other ephemeral identifiers such as a mobile number, IP address and domain name [14].

3. Proposed Governing Principles of Self-Sovereign Identity

Several IDM principles have been presented in the past in different contexts. Whether it was Kim Camerons Laws of Identity [15] or Christopher Allens Guiding Principles of SSI [16], they assisted the analysis of new and emerging SSI solutions and their success [17]. However, the (SSI) field is evolving rapidly as is the SSI requirements and standards [18]. Underlying these changing requirements, this section

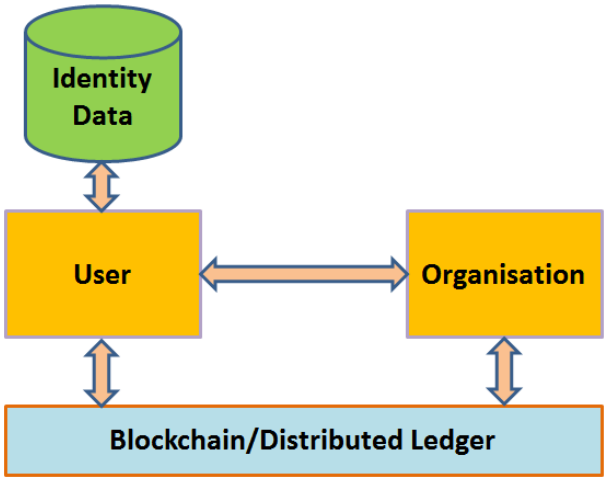

Fig. 4. Self-Sovereign Identity Management Model (IDM 3.0)

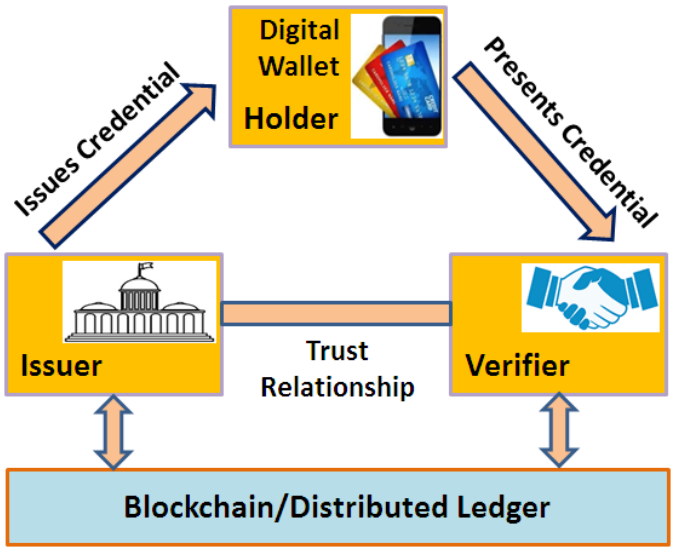

Fig. 5. Self-Sovereign Identity Ecosystem

proposes a revised and extended set of principles to analyse SSI solutions [10].

3.1. Sovereignty

An identity owner who owns an identity or identities must have the full sovereign control of their identity or identities, and it should not be controlled in any way by any other person, organisation or government. An identity owner should have all the necessary privileges for their identity or identities and be able to decide its correlation across different contexts without requiring any permission from any administrative authority or anyone else.

3.2. Existence of User

A digital identity can only be created for an existing user in the real world to represent them utilising selective information that is necessary for use in the cyber world. A user must have an independent existence prior to the creation of its identity and any identity cannot completely exist in the digital form without linking to the user. An identity simply ensures that certain aspects of an existing user are public and accessible.

3.3. Data Access Control

An identity owner who owns an identity or identities should have the full access control over their identity related personal identifiable information. An identity owner should be able to access, update, share, hide, or delete their identity related personal identifiable information. However, identity providers or authorised organisations can offer administrative support, which should not affect the access rights of identity owners.

3.4. Data Storage Control

All the identity related personal identifiable information should be owned and controlled by the identity owner. It should be stored and maintained on the storage, which is normally owned or controlled by the identity owner. Ideally, identity related personal identifiable information should not be stored on any externally controlled central repository or distributed ledger/blockchain.

3.5. Longevity

An identity must be eternal as long as its owner wishes, however, it can be revoked or abandoned by an identity owner. Therefore, an identity should be completely different from other ephemeral identifiers such as a mobile number, IP address and domain name. This longevity arrangement should be incorporated in underlying identity infrastructure and its operational model.

3.6. Decentralised

An identity should not be registered and managed centrally by any proprietary organisation. Digital identity should be registered and managed through a decentralised infrastructure mostly run publicly, such as distributed ledger technology or decentralised network technology.

3.7. Verifiability

An identity should be verifiable through its credentials in the cyber world in a way similar to a physical credential representing the real world identity. This could be digitally signed by the issuer and cryptographically secured; however, its verification may not necessarily require any interaction with its issuer.

3.8. Recovery

An identity infrastructure and services should be sufficiently resilient to successfully recover any identity in the event of a lost key, lost wallet or lost device. It should offer a number of mechanisms to identity owners to recover and re-assert their identities in the event of a complete loss of credentials. This means an identity should not be dependent on those artefacts, which can be lost, stolen, destroyed, and falsified.

3.9. Cost Free

An identity should be offered to everyone free of cost or absolutely negligible cost, without incurring any hidden cost, licensing fees, or any other financial charges for simply owning an identity. However, this may not apply to costs related to other resources and implementations. The cost factor is crucial if an identity should be offered to everyone on the planet.

3.10. Security

The security of an identity and its related communication is paramount for any identity infrastructure. It should include various security levels for identity such as cryptographically secure connections and communications, digitally signed transactions, and decentralized and encrypted storage.

3.11. Privacy

An identity owner should only be requested to provide or disclose the minimum identity information required for verification or service while maintaining as much anonymity as possible. The identity infrastructure should not provide any mechanism to correlate confidential and biometric data with an underlying identity. Any identity related personally identifiable information should only be shared after seeking the consent from its owner.

3.12. Safeguard

The freedom and rights of every identity owner should be safeguarded in all conditions. Accordingly, in the case of a conflict between identity owner and the identity network, the rights of an identity owner should be safeguarded independently. This is accomplished by employing an independent authentication system for an identity. This independent authentication system should be designed using sovereign tools and techniques, and free from any proprietary control.

3.13. Flexibility

An identity infrastructure and services should allow flexibility in nature of an identity by facilitating diverse, decomposable, extensible and gradual identity to users.

3.14. Accessibility

An identity infrastructure and services should be user-friendly and accessible by as many people as possible. This is of greater importance for non-technical and vulnerable people.

3.15. Availability

An identity infrastructure and services should be available to all without any discrimination based on their ethnicity, gender, socio-economic status, or language.

3.16. Transparency

All systems, protocols and algorithms employed in any identity infrastructure should be free, open-source, and as independent as possible of any particular architecture or proprietorship. Presently, the SSI community has been consulting on several open standards and forums to make this possible such as the Decentralized Identity Foundation (DIF), the World Wide Web Consortium (W3C) and the Organisation for the Advancement of Structured Information Standards (OASIS).

3.17. Portability

An identity and its related data should be easily transportable from one platform to another. This requires the standardisation of identity, credential and data formats.

3.18. Interoperability

Two different identity infrastructures should be capable of communicating with each other at scale. This will enable enterprises and government organisations to communicate with each other irrespective of their employed identity infrastructures.

3.19. Scalability

An identity infrastructure should be able to accommodate the increasing demand for a sovereign identity i.e. required for a large number of users, organisations and entities. This will determine the effectiveness of an identity infrastructure with respect to significant proliferation of digital entities in cyberspace.

3.20. Sustainability

An identity infrastructure and services should be environmentally, economically, technically and socially sustainable for the long term.

4. Comparative Analysis of uPort and Sovrin Ecosystems Based on the Proposed Governing Principles of SSI

Table I presents the comparative analysis of uPort and Sovrin SSI ecosystems based on the proposed governing principles of SSI. This comparative analysis shows that both uPort and Sovrin satisfy the major principles of SSI such as sovereignty, data access control, data storage control, longevity and verifiability which are fundamental requirements for SSI ecosystems [10], [13]. Furthermore, they support recovery, cost-free, security, privacy, safeguard, flexibility and accessibility principles; however, their degree of support varies with each principle, for example, Sovrin presently offers greater security and privacy features, whilst the uPort design architecture is simple and easy to use. The crucial commercial and operational principles of availability, transparency, portability and interoperability are yet to be fulfilled completely by uPort and Sovrin in order to establish them as a mature SSI ecosystem. As SSI is an emerging IDM model and uPort and Sovrin are emerging SSI ecosystems, therefore, the successful implementation of these commercial and operational principles

TABLE I
COMPARATIVE ANALYSIS OF UPORT AND SOVRIN SSI ECOSYSTEMS BASED ON THE PROPOSED GOVERNING PRINCIPLES OF SSI

Proposed SSI Principles	uPort SSI Ecosystems	Sovrin SSI Ecosystems
1. Sovereignty	It provides a sovereign identity.	It provides a sovereign identity.
2. Existence of User	It establishes the existence of user for creating an identity.	It establishes the existence of user for creating an identity.
3. Data Access Control	Identity owner fully controls identity related personally identifiable information.	Identity owner fully controls identity related personally identifiable information.
4. Data Storage Control	Identity and its related personally identifiable information is stored on the storage owned or controlled by the identity owner.	Identity and its related personally identifiable information is stored on the storage of an Edge Agent controlled by the identity owner, however, it may be stored on the storage of a Cloud Agent (protected from unauthorized access).
5. Longevity	It utilises a Decentralized Identifier (DID) which is a long-lived identifier.	It utilises a Decentralized Identifier (DID) which is a long-lived identifier.
6. Decentralised	It utilises a Decentralized Identifier (DID) which is a decentralised identifier.	It utilises a Decentralized Identifier (DID) which is a decentralised identifier.
7. Verifiability	It utilises Verifiable Credentials (VCs).	It utilises Verifiable Credentials (VCs).
8. Recovery	Social Recovery Method: Recovery Delegates (e.g. selected family members, friends or institutions) nominated by an identity owner, who can assist the user to regain its uPort identity.	Social Recovery Method: Recovery Key Trustees trusted by the identity owner store recovery data on their own agents on the behalf of an identity owner and help them to recover their identity.
9. Cost Free	Presently identity is free for users, however, all transactions have an inherent cost.	Presently identity is free for users, and no financial cost to identity transactions.
10. Security	It requires credentials and biometry for controlling identity through blockchain. Users can securely publish their identity including transfer their credentials, sign transactions and control their keys and data.	It requires credentials and biometry for controlling identity through blockchain. Users can securely publish their identity including transfer their credentials, sign transactions and control their keys and data using powerful cryptography.
11. Privacy	It is a Privacy Preserving. Users do not need to disclose personal data in order to create uPort identifiers for low value accounts. It uses various methods to minimize the correlation of a user's on-chain smart contract interactions between different dapps.	It is a Privacy by Design and Privacy by Default. It uses anonymous credentials based on Zero-Knowledge Proofs (ZKPs), which allows users to share the information that maintain the anonymity of users.
12. Safeguard	Users' right to privacy should be protected.	Users' right to privacy should be protected.
13. Flexibility	It provides flexibility in nature of an identity.	It provides flexibility in nature of an identity.
14. Accessibility	Simple design architecture and easy to use. At present it has no provision of a Guardian/Agent.	Complex design architecture and some users might require a Guardian to manage the identity on their behalf.
15. Availability	Users should require their smart-phone to manage their identity.	Users should require smart-phone but not necessarily its ownership.
16. Transparency	It is based on open standards and open source projects.	It is based on open standards and open source projects.
17. Portability	It is limited, however, uPort is using several open standards to make it portable, e.g., Verifiable Credential (VC) and Decentralized IDentifier (DID).	It is limited, however, Sovrin is using several open standards to make it portable, e.g., Verifiable Credential (VC) and Decentralized IDentifier (DID).
18. Interoperability	Presently it is evolving, therefore, it requires further alignment with other identity infrastructures.	Presently it is evolving, therefore, it requires further alignment with other identity infrastructures.
19. Scalability	It is limited. At present, the public Ethereum blockchain can process nearly 15 transactions per second. It is resolving this by avoiding creation of multiple smart contracts on the blockchain and allowing users to create Ethereum key pairs.	It is limited. At present, it is resolving this by using two rings of nodes: a ring of validator nodes to accept write transactions, and a much bigger ring of observer nodes to run read-only copies of the blockchain to process read requests.
20. Sustainability	It is an emerging SSI, therefore sustainability cannot be determined at this stage.	It is an emerging SSI, therefore sustainability cannot be determined at this stage.

require the development and adaptation of a set of common protocols and standards provided by standard organisations such as the Decentralized Identity Foundation (DIF), the World Wide Web Consortium (W3C) and the Organisation for the Advancement of Structured Information Standards (OASIS). Presently, the scalability principle is one of the important implementation issues for both uPort and Sovrin, it is being resolved by employing various design optimisation techniques to fulfil the growing demands of self-sovereign identity globally.

5. Conclusion

This paper proposed numerous governing principles of SSI for analysing any SSI ecosystem. Subsequently, based on the proposed governing principles of SSI, it performed a comparative analysis of two SSI ecosystems uPort and Sovrin to determine whether they comply with the proposed governing principles of SSI, presenting their effectiveness and limitations. In future, it is essential to analysing some other emerging SSI ecosystems based on the proposed governing principles of SSI.

References

[1] P. Windley. (2017) Fixing the five problems of internet identity. [Online]. Available: https://www.windley.com/archives/2017/10/fixing_the_five_problems_of_internet_identity.shtml

[2] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," *The Sovrin Foundation*, vol. 29, 2016.

[3] N. Naik and P. Jenkins, "A secure mobile cloud identity: Criteria for effective identity and access management standards," in *2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud 2016)*. IEEE, 2016.

[4] ——, "Securing digital identities in the cloud by selecting an apposite federated identity management from SAML, OAuth and OpenID Connect," in *11th International Conference on Research Challenges in Information Science (RCIS)*. IEEE, 2017, pp. 163–174.

[5] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena. (2018) Uport: A platform for self-sovereign identity. [Online]. Available: https://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf

[6] Sovrin.org. (2018) Sovrin: A protocol and token for self-sovereign identity and decentralized trust. [Online]. Available: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

[7] T. Ruff. (2018) The three models of digital identity relationships. [Online]. Available: https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186

[8] N. Naik and P. Jenkins, "An analysis of open standard identity protocols in cloud computing security paradigm," in *14th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2016)*. IEEE, 2016.

[9] N. Naik, P. Jenkins, and D. Newell, "Choice of suitable identity and access management standards for mobile computing and communication," in *2017 24th International Conference on Telecommunications (ICT)*. IEEE, 2017, pp. 1–6.

[10] N. Naik and P. Jenkins, "Self-Sovereign Identity Specifications: Govern your identity through your digital wallet using blockchain technology," in *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud 2020)*. IEEE, 2020.

[11] W3C. (2019) Verifiable Credentials data model 1.0. [Online]. Available: https://www.w3.org/TR/vc-data-model/

[12] ——. (2019) A primer for Decentralized Identifiers. [Online]. Available: https://w3c-ccg.github.io/did-primer/

[13] N. Naik and P. Jenkins, "uPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain," in *2020 IEEE International Symposium on Systems Engineering (ISSE)*. IEEE, 2020.

[14] Sovrin.org. (2018) Sovrin: A protocol and token for self-sovereign identity and decentralized trust. [Online]. Available: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

[15] K. Cameron, "The laws of identity," *Microsoft Corp*, vol. 12, pp. 8–11, 2005.

[16] C. Allen. (2016) Self-sovereign identity principles. [Online]. Available: https://github.com/ChristopherA/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md

[17] M. Graglia, C. Mellon, and T. Robustelli. (2018) The nail finds a hammer self-sovereign identity, design principles, and property rights in the developing world. [Online]. Available: https://www.newamerica.org/future-property-rights/reports/nail-finds-hammer/

[18] N. Naik and P. Jenkins, "Your identity is yours: Take back control of your identity using GDPR compatible self-sovereign identity," in *7th International Conference on Behavioural and Social Computing (BESC2020)*. IEEE, 2020.